DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

FIPS PUB 48

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION

1977 APRIL 1

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards

FEDERAL INFORMATION • FIPS • PROCESSING STANDARDS •

# *Guidelines*

# ON EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

U. S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, *Secretary*

Dr. Betsy Ancker-Johnson, *Assistant Secretary for Science and Technology*

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

## Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89–306 (Brooks Bill) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing systems in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of Government efforts in the development of guidelines and standards in these areas.

The subject areas of personal privacy, data confidentiality and computer security are of the greatest national interest. The Secretary of Commerce has identified the efforts required to provide solutions to technical problems encountered in these areas as personal objectives in the Department's overall program.

Data confidentiality and computer security are dependent upon the application of a balanced set of managerial and technological safeguards. Within the context of a total security program, the NBS is pleased to make this Guideline on Evaluation of Techniques for Automated Personal Identification available for use by Federal agencies.

Ruth M. Davis, *Director*
Institute for Computer Sciences
and Technology

## Abstract

This publication provides a guideline to be used by Federal organizations in the selection and evaluation of techniques for automatically verifying the identity of individuals seeking access to computer systems and networks via terminals, where controlled accessibility is required for security purposes. The guideline describes various techniques for verifying identity and provides a set of criteria for the evaluation of automated identification systems embodying these techniques.

Keywords: ADP security; computer networks; controlled accessibility; encryption; evaluation criteria; key; password; personal identification; terminals; verification.

Nat. Bur. Stand. (U.S.), Fed. Info. Process. Stand. Publ. (FIPS PUB 48), 22 pages (1977)

CODEN: FIPPAT

For sale by the National Technical Information Service,
U.S. Department of Commerce, Springfield, Virginia 22161.

Federal Information

Processing Standards Publication 48

1977 April 1

Announcing the Guideline on

# EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949, as amended, Public Law 89-306 (79 Stat. 1127), Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 Code of Federal Regulations (CFR).

**Name of Standard.** Guideline on Evaluation of Techniques for Automated Personal Identification.

**Category of Standard.** ADP Operations, Computer Security.

**Explanation.** This guideline describes methods for verifying the identity of users seeking to gain access to computer systems or networks via terminals. Criteria are given for evaluating the effectiveness of personal identification techniques. System considerations for inclusion as further safeguards to data confidentiality are indicated, as a supplement to personal identification.

**Approving Authority.** Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

**Maintenance Agency.** Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

**Cross Index.** Guidelines for Automatic Data Processing Physical Security and Risk Management, FIPS Publication 31; Computer Security Guidelines for Implementing the Privacy Act of 1974, FIPS Publication 41.

**Applicability.** This guideline is intended as a basic reference document for general use by Federal departments and agencies in the evaluation and selection of techniques for personal identification applicable for use with terminals.

**Implementation.** This guideline should be referenced by Federal agencies having requirements for controlling the access to computer systems and networks via terminals, where there is a need to verify the personal identity of terminal users.

**Specifications.** Federal Information Processing Standards 48 (FIPS 48), Guideline on Evaluation of Techniques for Automated Personal Identification (affixed).

**Qualifications.** A variety of techniques for personal identification are currently undergoing active development, resulting in rapid progress in this field. Accordingly, this Guideline stresses principles of the identification process and evaluation criteria, rather than specific methods of identification. Further research and testing is underway at NBS and other agencies and should lead to a more comprehensive understanding of the capabilities and limitations of available techniques. In this regard, comments and critiques concerning applications experience will be welcomed. These should be addressed to the Associate Director for ADP Standards, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234.

**Where to Obtain Copies.** Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia 22161. When ordering, refer to Federal Information Processing Standards Publication 48 (NBS-FIPS-PUB-48) and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, or deposit account.

Federal Information

Processing Standards Publication 48

1977 April 1

Announcing the Guideline on

# EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION

## CONTENTS

# EXECUTIVE OVERVIEW

The Privacy Act of 1974 (5 U.S.C. 552a) imposes numerous requirements upon Federal agencies to prevent the misuse of information about individuals and assure its integrity and security. These requirements will be met by the application of selected managerial, administrative and technical procedures which, in combination, can be used to achieve the objectives of the Act.

This Guideline discusses techniques for the identification of individuals for the purpose of controlling access to computer networks. Measurement of the effectiveness of personal identification devices is described and evaluation criteria are presented as a guide in comparing and selecting appropriate techniques and devices.

There are three general bases on which the identity of an individual may be verified, namely, something known by the individual, something possessed by the individual, or something about the individual (physiological attributes, such as fingerprints, hand geometry, signatures, and voice prints). These three categories are discussed in the Guideline, together with system considerations and possible forms of compromise. The distinction between intrapersonal and interpersonal variability is pointed out.

The performance of devices based on physiological attributes may be less than ideal, and a compromise may be necessary between the possible rejection of a small percentage of authorized individuals and the acceptance of a small percentage of unauthorized individuals. Devices may generally be adjusted for a trade-off between these two categories, such that the most important category for a particular application may be emphasized at the expense of the other category. Greater certainty may be achieved by combining two or more methods of identification, provided that the appropriate decision rules are employed, and this subject is considered in the Guideline.

Accurate verification of the identity of an intended user does not completely eliminate the risk of unauthorized access, since an authorized individual might be persuaded to gain access on behalf of an authorized individual through collusion or extortion, or he might carry out an unauthorized activity for reasons of his own. The Guideline discusses other provisions for countering these threats which can be incorporated in a system for use as adjuncts to the personal identification techniques.

# GUIDELINE ON EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION

## 1. Introduction

Attention has recently been focused on computer security and the safeguarding of data confidentiality for the purpose of protecting personal privacy. This has emphasized the need for accurately establishing the identity of individuals authorized to have access to computer systems. There is a recent legislative mandate for this need, within the Federal Government, as embodied in the Privacy Act of 1974 (5 U.S.C. 552a). Through this law, the Congress has asserted that "the privacy of an individual is directly affected by the collection, maintenance, use and dissemination of personal information by Federal agencies." Congress has further recognized the potential of the computer to be used for intruding upon individual privacy and has laid down requirements for regulating the handling of personal information within the Government[17].[1]

Control of access to computer systems and networks is becoming increasingly important as computers are entrusted with more sensitive applications and more valuable information. Much emphasis has been placed in recent years on increasing the accessibility of the computer in order to accommodate the user and to enhance his ability to interact with it. This has posed new threats to system security and has emphasized the need for moer adequate safeguards against unauthorized access and the misuse of computer resources [1, 11, 19].

### 1.1. Need for Personal Identification

Central to the implementation of safeguards required by the Privacy Act is the ability to establish the identification of individuals: individuals who operate computers, write programs for computers, prepare and enter data, enter queries, receive output, and those who repair computers [4, 9]. For a broader treatment of security system implications of the Privacy Act, the reader is referred to Computer Security Guidelines for Implementing the Privacy Act of 1974, FIPS PUB 41 [18].

This Guideline considers a number of approaches to providing protection against unauthorized access by verifying the identification of individuals seeking to access computer systems. The emphasis is upon approaches, rather than upon specific devices. A set of evaluation criteria is given for assessing and comparing the suitability of alternative identification devices.

### 1.2. "Absolute" Identification Versus Verification of Identification

A distinction should be drawn between carrying out an "absolute" identification as opposed to simply verifying an identification. In an "absolute" identification, a determination is made as to the identity of an individual, independently of any information supplied by the individual; the individual may be uncooperative, and in fact may be unaware that his identity is being sought. For example, a set of fingerprints might be obtained from a suspect apprehended under suspicion; these could then be sent to a fingerprint technician to be classified, and then a file could be searched until a match was obtained. The identity of the individual could then be obtained from the card containing the matching set of file prints.

The personal identification process, as considered in this Guideline, is more properly considered identity verification. In this process, a would-be terminal user is assumed to be cooperative and presents a claimed identity to the system. The individual is then required to carry out a certain "procedure" which provides the system with the data necessary to either confirm or refute the claimed identity. This process compares a set of data derived from the individual with the corresponding set of data retrieved from a file or other source, based on the claimed identity. If the two sets of data can be matched within a certain tolerance, the identity is considered to be verified. It should be noted that this verification process does not require an extensive searching process as might be required for a true identification process.

[1] Figures in brackets indicate the literature references at the end of this paper.

## 2. Three Basic Methods of Establishing Identity

There are three basic methods by which the identity of an individual may be established:

(1) Something KNOWN by the individual;

(2) Something POSSESSED by the individual;

(3) Something ABOUT the individual [2].

The first category includes such things as a password, the combination to a lock, or facts from an individual's personal background. The second category includes artifacts, such as badges, passes, cards with machine-readable information, and keys to locks. The third category includes physiological attributes, such as an individual's appearance, voice, fingerprints, and hand geometry.

### 2.1. Something KNOWN to an Individual

Verification of identity through the use of an item of information known only to an individual, or to a limited set of individuals, is exemplified by the password. Passwords are presently the most commonly used method of controlling access to time-sharing systems. This method can be extended to provide for multiple passwords and question-and-answer sequences. The latter would typically include a random subset of items selected from a file of known information, such as names of family members, schools attended, teachers, events of personal history, or other facts.

Of course, anything known by one individual may become known by another, who may then succeed in an attempt at impersonation. In assigning passwords, it is preferable for each user to have his own password, rather than to use the same password for a set of users. Whenever a system is accessed, it should keep a log of the password used and the nature of the access. This permits the activities of various users to be audited. In the event that an unauthorized activity should come to light, this audit trail would indicate the password that was involved and would point toward the possible culprit. With individual passwords, an individual could not allow his password to be used by an accomplice without exposing himself to suspicion. Or, if a password were stolen, the likely source would be evident and steps could be taken to achieve increased security awareness. Individual passwords can be used by the system in controlling access by users to specific system resources, including information files and applications.

The generation of passwords ideally should be done under centralized control [3]. The selection of passwords should avoid any obvious bases, such as the individual's middle name or initial. In some cases, it might be desirable to generate passwords by a random process, though in this case the use of a known algorithm which generates pseudorandom data should be avoided. (A true random process would occasionally produce duplicate passwords; this can be avoided by using a technique such as sampling without replacement.) Passwords should be as long as feasible, consistent with requirements for memorization and use, thus reducing the possibility of determining them by trial and error. Passwords should be changed at intervals, and at any time that they are suspected to have been compromised.

A log should be kept of such changes showing the date of change, new password, and authority. The authorizing official should sign the log personally each time a change is made.

The degree of security provided by the password (or the combination to a lock) is largely dependent upon the possible number of combinations from which it is chosen [13]. As a very elementary case, consider a password which consists merely in flipping a coin. Assume that if the coin comes up "heads," access will be granted, but if it comes up "tails," access will be denied. What is the probability that a would-be user would be granted access on the basis of a single toss of the coin? Since there are only two possibilities, both equally probable, he has a 50 percent chance of being successful. If he were to seek access on a number of occasions, he would be successful half the time, on the average. Now suppose that for each attempted access, two successive tosses were required, and that access would be granted only for the sequence "heads-heads." There are now four possible combinations, only one of which is valid, so the possibility of gaining access by chance is reduced to 25 percent. By extension, the change of achieving the right combination for a sequence of $n$ tosses is 1 in $2^n$.

Suppose, now, that instead of a coin, the would-be user is required to use dice. Since a die has six sides, instead of two, the previous expression becomes 1 in $6^n$. Now consider a combination lock having $n$ dials, each divided into 10 steps.. The expression for this case is 1 in $10^n$. Many combination locks have a single dial with perhaps 50 to 100 steps, but a series of right and left rotations are required to dial the full combination. The expression for such a lock would be more complex but basically would be obtained by similar reasoning.

Now consider a password consisting of $n$ letters chosen from the 26 letters of the alphabet. It would appear that the chance of achieving such a combination by chance is 1 in $26^n$. However, this is greatly reduced if the number of allowable combinations is constrained in some manner. Are the passwords to be pronounceable? Then perhaps every second or third letter is a vowel, of which there are only 5. Consider an elementary password consisting of 3 letters chosen at random from an entire alphabet; the number of such combinations is $26^3 = 17{,}576$. But suppose this is restricted to combinations consisting of consonant-vowel-consonant. The number of such combinations is $21 \times 5 \times 21 = 2205$, or about one eighth as many as before. If the choice of passwords is further restricted to valid words and names in the language, a still more drastic reduction in the number of combinations occurs.

There is another way in which this phenomenon of reduction in combinations can occur. Consider that the letters of the alphabet are being used, but that they are being typed on a keyboard and that each character is represented by a seven-bit code. Each character of code would be capable of representing $2^7 = 128$ combinations, yet only the 26 combinations representing the alphabet are being employed in this case. Thus, for a string of $n$ characters, the allowable combinations would be $26^n$, whereas the number of combinations that could be realized with this many seven-bit characters would be $128^n$ or about $5^n$ times as many combinations.

In assessing the security of a given password scheme, it is important to consider the number of allowable combinations for valid passwords, rather than the theoretical number of combinations which might be obtainable based on the number of symbols and the length of the sequence employed. The more characters a password contains, the more combinations are possible; however, this is likely to increase the difficulty of memorizing and using it and may increase the likelihood of its being written down in a convenient place.

Systems employing passwords should be designed in such a way that the passwords can be entered in a concealed manner. It should not be possible to discover a password simply by obtaining a scrap printout from the trash. Defenses employed against this latter threat include the following:

(1) On hardcopy (printing) terminals the password may be obscured by automatically overprinting (or underprinting) several times in the area where the password is to be typed.

(2) On a softcopy (CRT) terminal the screen may be immediately erased upon entry of a character or password.

(3) On either a hardcopy or softcopy terminal operating in a full duplex mode the password may be kept from appearing by not echoing it.

(4) The password may be kept from appearing by using a sequence of non-printing (or non-displayed) characters, although such a sequence might be more difficult to remember than an alphanumeric sequence.

There is a certain risk of exposure at the time that a password is actually entered. For example, the user might be observed entering the password, or it might be obtained by a wiretap. Encrypting the data between the terminal and the computer can protect against the wiretap threat. Another possibility is to use one-time passwords. For this, the users are given lists of passwords and choose the next one in succession for each use. Alternatively, they could be supplied with a new one after each use (assuming that a secure method of delivery were available). The advantage of one-time passwords is that any password which might be observed or intercepted would not be usable by an intruder for another access.

## 2.2. Something POSSESSED by an Individual

Locks and keys constitute a familiar access mechanism and one which is frequently associated with operator's consoles and maintenance panels. Computer terminals have also been fitted with locks. The degree of security afforded by a lock and key is limited, however, since a key can be lost or stolen, and many locks are not difficult for an expert to pick. If a key falls into the hand of an unauthorized person, it may be necessary to rekey the lock, which can be a nuisance. Further, the key might be duplicated and returned by an unauthorized person, without the owner being aware of its loss. Thereafter, unauthorized access could be gained without anyone realizing that it was taking place.

More sophisticated means of access control are becoming available, usually in the form of a card having some type of machine-readable data encoded on it. The data are generally represented in such a manner as to be difficult for a would-be counterfeiter to read, interpret, or duplicate. Provisions can be included for assigning unique codes to individuals and sets of individuals. The reading stations for these cards can be controlled in a manner which permits the stations to be selectively operated by specific cards, accepting those which are authorized and excluding those which are not; also, access can be denied to cards which are "delisted" (removed from the authorization list). A list of cards for which access is to be denied is called a negative list. The card may include a picture of the individual for use in situations where visual identification is employed. Various technologies for embedding coded information in cards are being used or are under consideration, such as the embedding of patterns of magnetic materials, patterns of materials which can be sensed by infrared or x-ray radiation, and electronic circuitry which either produces or responds to radio frequency radiation. There may be provisions for variable data which can be altered with each use, providing a degree of security similar to one-time passwords.

Techniques such as encryption and scrambling may be used in connection with cards and the devices that read them in order to further enhance their security by making it difficult to read or interpret the data contained on them and to protect the transmissions between the reading device and the system being accessed. (See Section 6.5.) If the card is to contain an image that would normally be recognizable, such as a signature or picture, this may be recorded through a special lens system which creates an unrecognizably scrambled image. The scrambled image can only be read by viewing it through the inverse lens system which restores it to its original form.

The problem with a key or a card or other artifact is that it could fall into the hands of an unauthorized user through loss, theft, or other means. Therefore, it may be necessary to provide additional methods of verification where a higher level of security is required.

### 2.3. Something ABOUT an Individual

Because of the vulnerability of other methods of identification to such threats as theft and duplication, much emphasis is presently being focused on the technology of personal identification through physiological and morphological attributes [10, 11]. Among those which are in use or under consideration are faces, signatures, fingerprints, hand geometry, voice-prints, ear features, dental characteristics, prints from the bottom of the feet, and patterns on the retina of the eye. Another method obtains a dynamic muscular-skeletal response function by applying a mechanical stimulus at one point on the body and observing the resulting signal at another. The use of attributes of this type for personal identification is discussed in the next section.

## 3. Personal Identification by Means of Physiological Attributes

Consideration has been given to a variety of physiological atributes as possible bases for personal identifiaction, as listed in the preceding section.

Because of various limitations and drawbacks in the current state-of-the-art, much effort is presently being expended in the search for an ideal choice of attribute(s) and recognition technology. A key consideration is the degree of intrapersonal variation versus interpersonal variation. Intrapersonal variations are those exhibited by a given attribute for a specific individual from one measurement to the next, considering various influencing factors including the passage of time. Interpersonal variations are those exhibited from one individual to another. Intrapersonal variations make it necessary to allow tolerances in the recognition process. But, as these tolerances are made larger, the likelihood of one individual being able to impersonate another is increased, which could raise the probability of an imposter being accepted.

A substantial problem in the use of physiological attributes is the difficulty of performing precise, repeatable measurements. Because of the curvilinear nature of the body surfaces and the plasticity of body tissue, it is difficult to establish accurate reference points and good registration for the purpose of taking measurements or pattern matching. Fingerprints are highly deformable, depending upon pressure both normal and tangential to the surface. There are topological relationships that are preserved under such deformations, and a trained analyst can pick these out, but it becomes much more difficult to achieve machine recognition under these circumstances.

Lack of precise repeatability is characteristic of most physiological attributes and processes, including handwriting and speaking. This must be taken into account in testing and evaluating a candidate identification system. In performing such tests, provision should be made to vary all factors that are considered to have an influence on the attribute(s) being utilized.

### 3.1. Appearance

People are most frequently identified by their faces, and this method of identification is embodied in the picture pass or badge which bears a black-and-white or color photograph of the individual. This method is not applicable to remote terminals unless the terminals are kept in areas to which access is controlled by guards [16]. Equipment is available for transmitting facial images by means of closed-circuit television from a terminal area to a manned central location where a picture file of authorized individuals is maintained. An individual to be identified furnishes his claimed identity and presents himself to the television camera, whereupon a file image is retrieved and compared by a guard with his "live" image on a monitor screen. If the guard is convinced that these images are alike, the identity is considered to be verified. This method is constrained by the need for a high bandwidth channel from the remote site to the central site, in order to convey the television images, and the comparison must be performed by a human. A slow-scan television system might be used to lower the bandwidth requirement, but this could lengthen the time to transmit the image and might reduce the resolution of the image.

### 3.2. Signatures

Signatures are frequently used as one method of verifying personal identity and for the authentication of documents. While handwriting, in general, tends to have unique characteristics from one individual to another, the signature is even more unique, since it is practiced frequently over a lifetime, often becoming highly stylized. Equipment for automatically comparing signatures is under development and appears promising as a means of personal identification [12]. While it would be possible to develop equipment for comparing completed signatures as static patterns, this would be vulnerable to deceit, either through forgery or the entry of a copy of the signature. A more promising approach is to make use of an instrumented stylus which senses the dynamic motions (velocity, acceleration, pressure) which occur during the actual signing process. These motions are highly characteristic of the individual and would be extremely difficult for an imposter to perceive or duplicate. It appears that sufficient information for the identification process can be obtained by extracting as little as a few dozen samples during the signing process. A typical signature takes 4 to 5 seconds; to this must be added the time to pick up the stylus and respond to a starting signal, and the time for the device to determine that the signature is completed. This extends the signing process to about 8 seconds. This data rate is sufficiently moderate to permit transmission to a central location where the matching process can be performed using a reference signature profile obtained from a central file. Note that the identification process simply consists of matching the profile of the "live" signature with the reference profile obtained from storage; it is not necessary to recognize the individual letters making up the signature (which would frequently be impossible). In using this method of personal identification, the individual would enter a claimed identity (and such other information as might be required) and then sign his name, using the instrumented stylus or tablet. The claimed identity would be used to retrieve from storage the reference profile to be compared against the profile of his "live" signature. If they matched to within some tolerance, his identity would be considered to be verified.

In principle, other words could be selected in lieu of the signature, and profiles of these words could be placed in storage for matching purposes. However, there are unique qualities in the way a signature is written, having the nature of a conditioned reflex, which cause it to be preferable to ordinary handwriting for identification purposes.

### 3.3. Fingerprints

The use of fingerprints is one of the most well-established systems of personal identification currently in use [6]. However, fingerprints are not generally used for real-time applications because of the time and effort consumed in obtaining good images which are easy to view and because of the training needed for making comparisons. Much effort is being expended to overcome these difficulties, and terminal-oriented recognition systems based on fingerprints are beginning to emerge.

Two basic approaches are being pursued in automating the matching of fingerprints. One method consists of a direct optical comparison between the "search" print (the print being entered) and the file prints. In the other method, the search print is scanned and a list of significant detailed features ("minutiae") is compiled in digital form. This list may then be compared with a similar list for the file print [13].

In a personal recognition device using the direct optical comparison method, the comparison process must be carried out locally within the recognition device, since it is not practical to transmit the fingerprint image over a distance. One way of obtaining the two images to be compared is to have a card containing the file copy of the fingerprint entered into the device along with a card containing a fresh print of the corresponding finger. Sensitized material is available for producing a visible image from a fingerprint directly, without the need for inking of the finger. Alternatively, the user might key in identifying information which would cause the file print to be retreived from an internal file and positioned in the recognition device. He could then enter a card containing his fingerprint to be compared with the file print. Within the device, the images of the search print and the file print are compared using optical correlation, and an output signal is produced signifying the degree of match obtained. Since it is difficult to establish a precise reference for aligning fingerprints, the device will generally include a means for rotating one of the images slightly in order to allow for misorientation. Experimental work with holographs is being carried out for use in fingerprint matching systems.

In the digital comparison method, the person keys in identifying information which causes the minutia list for his fingerprint to be retrieved from a file at a central location. He then places the corresponding finger on an optical window and a scanning process is performed to develop a search minutia list from the "live" print. The search minutia list, which requires only a moderate amount of data, is sent to the central location, where a comparison is carried out between the search minutia list and the file minutia list, using special algorithms for this purpose. Because of alignment problems and the plasticity of the finger, it is generally not possible to get an exact match, but the comparison process develops a score which indicates the likelihood that the two prints are the same. The central system may have minutia lists on file for more than one fingerprint for a given individual, in order to allow for the possibility that the first finger to be tried might not be scanned properly for some reason such as an injury.

### 3.4. Hand Geometry

The shape of an individual's hand has been found to exhibit sufficient interpersonal variability to serve as a basis for personal identification. Equipment has been developed which senses the lengths of the fingers, translucency of the web between the fingers, and curvature of the finger tips. In a commercial device for this purpose, the individual to be identified carries a card with identifying information plus the data representing the profile of his hand measurements. The data is represented in scrambled form. He inserts the card into the recognition device and then positions his hand upon the sensing area. The finger measurements are then derived from his hand and compared with the data read from the card. If a match is obtained, his identity is considered to be verified. This complete process can be done in less than three seconds. Alternatively, the profile data may be stored centrally. In this case, the individual first supplies identifying information to the system and then positions his hand upon the sensing area. The finger measurements are then transmitted to the central location for comparison with the profile data. The system can then respond appropriately, based upon whether or not a match is obtained.

### 3.5. Voiceprints

Patterns of spoken words have been found to exhibit characteristics which are sufficiently unique to serve as a basis for personal identification. Graphical images of spoken words may be formed by means of equipment which plots energy at different frequencies as a function of time. The resulting patterns are called voiceprints and have been studied extensively. Expert analysts are required to compare one voiceprint with another. Waveforms of spoken works may be digitized and fed into a computer for analysis and comparison. Development work of this type is being actively pursued as a means of enabling spoken data to be entered directly into computer. Development work is also proceeding on equipment for automatic speaker verification [5]. The use of speech as a method of personal identification is attractive because speech can readily be transmitted over long distances by telephone, enabling the recognition equipment to be at a central location. Transmission by telephone has a significant effect upon speech waveforms, although there are certain features which tend to remain invariant or to change in a predictable manner. Voice characteristics can be influenced by an individual's health, emotional stress, and other factors, which might interfere with the recognition process.

### 3.6. Other Attributes

The attributes considered thus far are the ones which currently appear to offer the most promise for application to remote personal identification. Those attributes listed in Section 2.3 which have not been discussed are felt to be either less developed, less convenient to use, or less promising for remote application. It should be noted that this is a very active field, because of the current emphasis on security, and that the relative merits of competing methods may shift as developments proceed.

## 4. The Accept / Reject Decision

Devices for personal identification based upon physiological attributes generally operate in the following manner:

(1) The would-be entrant or user instructs the device as to who he purports to be. He may do this by keying in his name or a personal ID number or other identifier. Or, he may insert an artifact, such as a magnetic striped card having such information.

(2) The device then prepares to verify the claimed identity. This will be done by compar-

ing a reference profile of the physiological attribute for that individual with the measured profile of the attribute as derived from the individual. Depending upon the device and the application, the reference profile may be obtained from a central file, it may be obtained from a local file in the device, or it may be read from an artifact supplied by the individual. An alternate method is to measure the attribute and send the measured profile to a central location for comparison with the reference profile.

(3) The measured profile is compared with the reference profile and the degree of correlation is obtained. This generally results in an output signal from a comparator having a value lying between some minimum and maximum value.

(4) The resulting value is compared with a preset threshold which results in a binary decision to accept or reject the individual.

Due to the compromises which arise in realizable recognition devices, the decision process is generally subject to some degree of imperfection and this can manifest itself in two forms:

Type I errors: rejection of an authorized individual; this is quantified as the False Alarm Rate (FAR).

Type II errors: acceptance of an imposter; this is quantified as the Imposter Pass Rate (IPR).

In statistical treatments, the probabilities associated with Type I and Type II errors are usually designated $\alpha$ and $\beta$, respectively [21].

### 4.1. Determination of False Alarm Rate (FAR)

The FAR indicates the degree to which the identification device fails to recognize authorized individuals. A FAR of 2 percent would indicate that authorized individuals would be rejected in two attempts out of 100 (on the average); that is, the device would generate a "false alarm," implying that the individual is an imposter when in fact he is not. The method of determining the FAR for an identification device is to select a population, enlist the members of this population as authorized individuals, train them in the operation of the device, and then carry out a planned test in which each member attempts to identify himself through the device one or more times. For each attempt, the response of the device is noted, namely whether the individual was accepted or rejected. It is also extremely valuable to record the value of the comparator signal produced within the device, if it is available, in order to have a quantitative indication of the margin by which the decision threshold is exceeded. (See Figure 1)

The FAR is calculated from the test observations as follows:

FAR = (Number of False Rejects) divided by (Total Number of Identification Attempts for Authorized Persons)

The size of the population and the number of trials per individual would be based upon the degree of confidence desired in the determination of the FAR. Statistical techniques are available for the design of experiments of this type. [15]. The FAR may be found to vary from one individual to another in a given population; that is, certain individuals may exhibit higher FARs than the population as a whole, indicating that these individuals are less consistent with regard to the attribute used for verification.

The design of a test for determining the FAR of a particular device should take into consideration any variable factors which might influence the performance of the device, such as an individual's physical state (rested, tired), the effects of exertion, emotional stress, whether before or after meals, time of day, room temperature and humidity. A knowledge of the principles of operation of the specific device would be important in deciding what factors might influence its operation.

As discussed previously, there are various considerations which cause the operation of identification devices to be less than ideal (intrapersonal variation, deformability of tissue, etc.). This means that an authorized individual may occasionally be rejected on any given attempt. The probability of this is expressed by the FAR. This shortcoming can be offset by allowing the individual to repeat the identification attempt. The number of such attempts should generally be limited to a low value, such as three, in order to prevent an imposter from trying to thwart the device through some repetitive form of deceit. The FAR gives an indication of the number of occasions on which multiple attempts would be required. With a FAR of 5 percent, an authorized individual would be rejected once out of every 20 attempts, on the average. However, by making further attempts he should be correctly recognized. Some test data indicates that an individual may occasionally be found to have deviated beyond the tolerance for acceptance. In such cases it may be necessary to re-enroll the individual.

In evaluating the performance of an identification device it is helpful to plot the test data as shown in Figure 1.

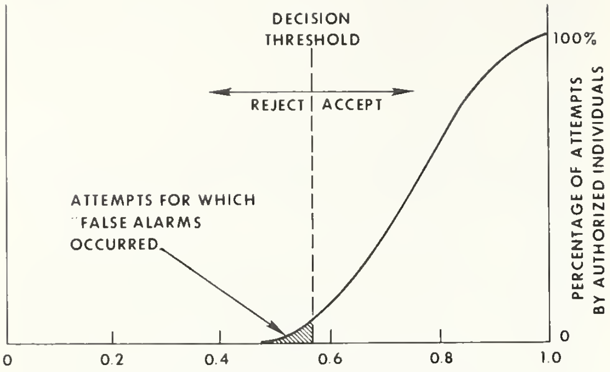

FIGURE 1
PLOT OF EXPERIMENTAL DATA OBTAINED IN
CONDUCTING THE TEST FOR FALSE ALARM RATE (FAR)

### 4.2. Determination of Imposter Pass Rate (IPR)

The IPR indicates the degree to which the identification device fails to reject imposters. An IPR of 3 percent would indicate that, on the average, imposters would be accepted in three attempts out of 100.

The IPR is intended to reflect only those situations in which the acceptance of an imposter is coincidental; that is, the imposter makes no active effort at deceit, other than to falsely claim to be an authorized individual. It should be evident that, with sufficient ingenuity and effort on the part of the imposter, a substantially higher IPR might be achieved. This is considered further in the discussion of evaluation criteria. The method of determining the IPR for an identification device is to select a population, train the members of this population in the operation of the device, and then carry out a planned test in which each member attempts to identify himself to the device one or more times, while purporting to be an authorized user (other than himself). The sample population chosen for this test may include individuals who have established authorized identities with the device; however, for this test they attempt to impersonate authorized individuals other than themselves. For each attempt, the response of the device is noted, namely whether the individual was accepted or rejected. It is also very valuable, as with the FAR test, to record the comparator signal produced within the device.

The IPR is calculated from the test observations as follows:

IPR = (Number of False Acceptances) divided by (Total Number of Identification Attempts for Imposters)

As with the FAR test, the size of the population and the number of trials per individual would be based upon the degree of confidence desired in the determination of the IPR [15]. Again, any variable factors which might influence the performance of the device should be taken into consideration in the design of the test.

In evaluating the results of this test, it is helpful to plot the test data as shown in Figure 2.

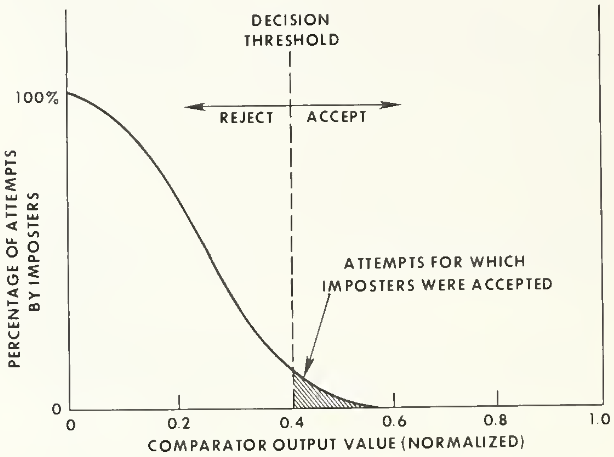

FIGURE 2
PLOT OF EXPERIMENTAL DATA OBTAINED
IN CONDUCTING THE TEST FOR IMPOSTER
PASS RATE (IPR)

The FAR data and the IPR data are generally plotted on the same graph, as shown in Figure 3.

### 4.3. Combined Test for FAR and IPR

In practice, it is more practical to employ a single composite test design for determining the FAR and the IPR, rather than testing for them separately. In order to keep the statistics unbiased, the observers should be unaware of whether a particular attempt is being made by an authorized individual or an imposter.

The preferred performance of an identification device would be such that the regions portrayed in Figure 3 were clearly separated as in Figure 4. This performance data exhibits a region in which the comparator signal never occurs; by adjusting the decision threshold to lie within this region, the FAR and IPR could both be reduced to zero. The device would then accept all authorized persons and reject all imposters.

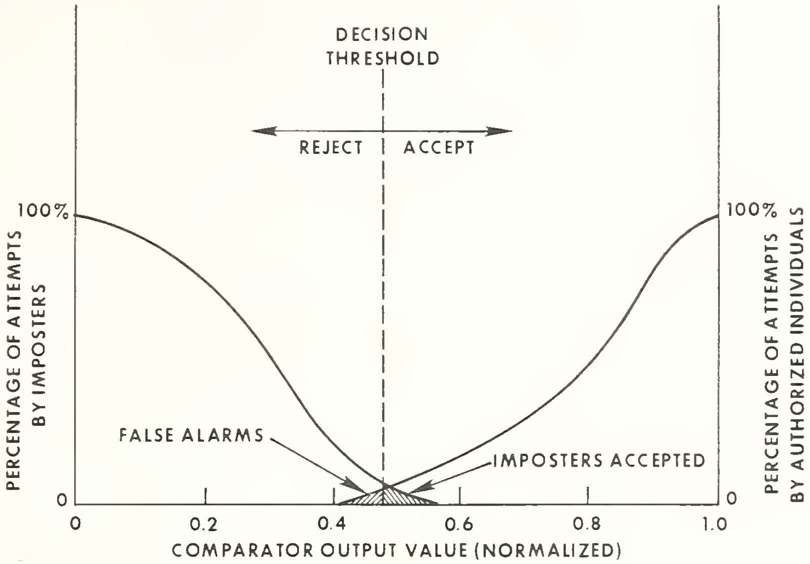

FIGURE 3
FAR DATA & IPR DATA PLOTTED ON SAME GRAPH

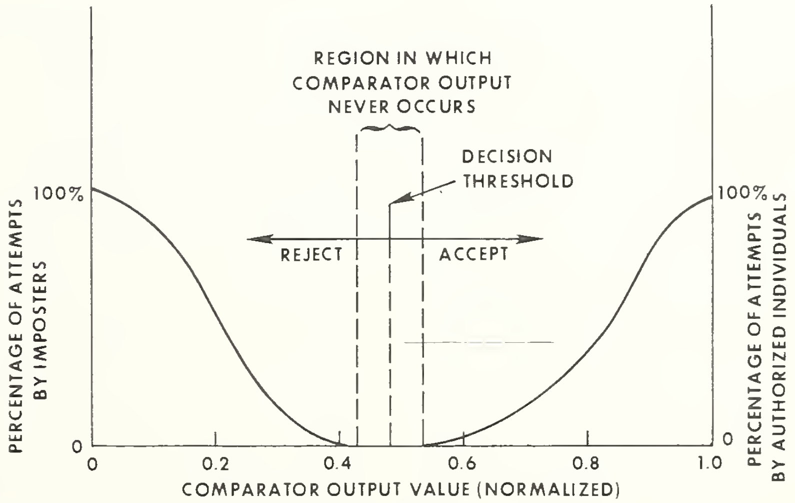

FIGURE 4
PREFERRED PERFORMANCE OF
IDENTIFICATION DEVICE

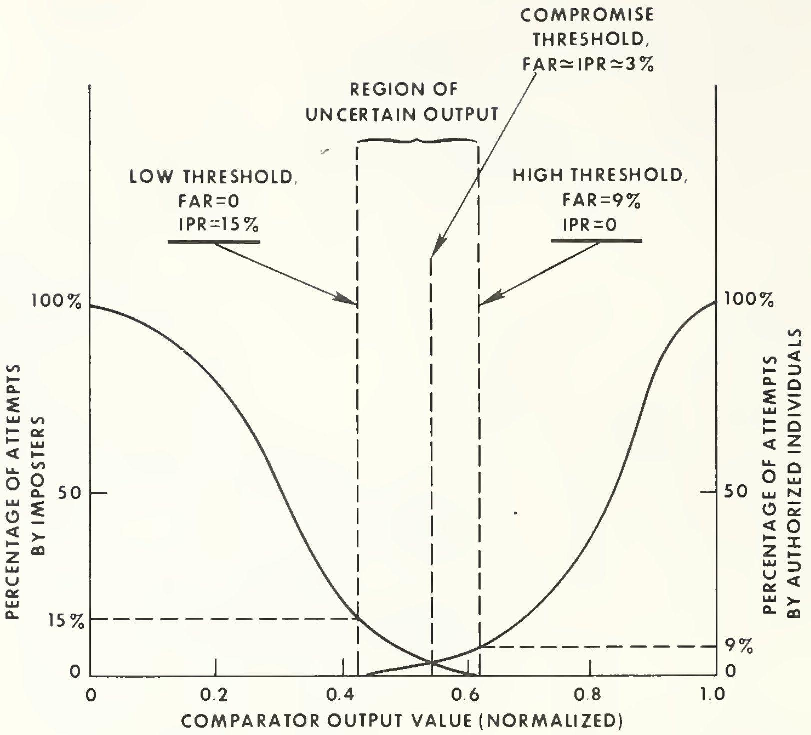

FIGURE 5
TYPICAL PERFORMANCE OF A REALIZABLE IDENTIFICATION DEVICE

In practically realizable identification devices, a certain amount of overlap is generally encountered, as shown in Figure 5.

In such cases, the setting of the decision threshold must be a compromise. If one of the factors is of greater concern than the other, the threshold can be adjusted to reflect this. For example, if rejection of imposters is the main objective, a higher threshold setting can be used, reducing the IPR to zero but increasing the FAR. Another possibility is to establish two thresholds for the comparator output, to be interpreted as follows: If the high threshold is exceeded, it is certain that the individual is authorized; if the output is below the low threshold, it is certain that the individual is an imposter; if the output is between the two thresholds, an uncertainty exists and an alternative procedure should be invoked to verify the identity.

### 4.4. Effect on FAR and IPR of Allowing Multiple Attempts

Where a personal identification system exhibits a nonzero FAR value, it is generally necessary to allow an individual more than one attempt to verify his identity. However, it should be noted that the effective FAR and IPR values are significantly affected by allowing multiple attempts. Consider a system with a basic FAR of 3 percent and an IPR of 2 percent. On the basis of single attempts, authorized individuals would be rejected 3 percent of the time. By allowing a second attempt, the probability of being rejected twice would be 0.03 × 0.03 or 0.0009, or less than once in a thousand. (This assumes that the performance of the device is statistically independent for each attempt. In practice, it may be found that some individuals experience more difficulty than others, so the effective FAR improvement might not be quite as great as indicated.) In order to realize this enhancement of the FAR, it must be assumed that the individual will be accepted if he is successfully verified on **either** attempt. Applying this rule, the IPR would increase in proportion to the number of attempts allowed. Assuming the performance of the device to be statistically independent for each attempt, a basic IPR of 2 percent would become approximately 4 percent for two attempts, 6 percent for three attempts, and so one. (If **p** is the probability of an imposter being accepted in a single attempt, the probability of his being accepted at least once in n attempts is $1 - (1 - p)^n$, which for small values of $p$ is approximately proportional proportional to the number of attempts.) Therefore, if multiple attempts must be allowed in order to realize an acceptably low effective FAR, then a correspondingly lower basic IPR will be required in order to keep the effective IPR with multiple attempts from becoming excessive.

### 4.5. Combining of Personal Identification Methods

The accuracy of the personal identification process may be enhanced by combining two or more methods, rather than relying on a single method. However, attention must be given to the decision rules which are used in combining the results of the separate methods. Various alternatives are shown in Table 1, in which two identification methods are employed jointly. Method 1 is assumed to have $\text{FAR}_1 = 5$ percent and $\text{IPR}_1 = 8$ percent. Method 2 is assumed to have $\text{FAR}_2 = 7$ percent and $\text{IPR}_2 = 12$ percent. It is assumed that the methods are statistically independent of each other in their performance.

Consider Alternative A of Table C1. This rule states that the individual is to be accepted only if he is accepted by both Method 1 and Method 2. This has the effect of strengthening the rejection of imposters, resulting in a joint IPR which is the product of $\text{IPR}_1$ and $\text{IPR}_2$; $\text{IPR}_A = 0.96$ percent. However, the likelihood of an authorized individual being rejected is now gerater than for either method alone, the joint FAR being approximately the sum of the FARs for the separate methods: $\text{FAR}_A = 12$ percent. Statistical independence is a reasonable assumption in this case.

Under Alternative B, the individual is to be rejected only if he is rejected by both Method 1 and Method 2. This cuts down on false alarms at the expense of increasing the acceptance of imposters. Under this alternative, $\text{FAR}_B$ is 0.35 percent while $\text{IPR}_B$ is about 20 19 percent.

It is possible to realize improvements in both the FAR and IPR by establishing the rule that an individual will be accepted or rejected only if both systems are in agreement, as shown in Alternative C. In this case, different identification procedures are to be invoked for situations in which the two methods give contradictory results. Under Alternative C, if an individual experiences a contradictory result (as indi-

TABLE 1

| Method 1 | Method 2 | Alternative Decision Rules | | |
|---|---|---|---|---|
| $\text{FAR}_1 = 5\%$<br>$\text{IPR}_1 = 8\%$ | $\text{FAR}_2 = 7\%$<br>$\text{IPR}_2 = 12\%$ | Alternative<br>A | Alternative<br>B | Alternative<br>C |
| Response | Response | Decision | Decision | Decision |
| Accept | Accept | Accept | Accept | Accept |
| Accept | Reject | Reject | Accept | * |
| Reject | Accept | Reject | Accept | * |
| Reject | Reject | Reject | Reject | Reject |
| | | Effective Values for Combined Systems | | |
| | | $\text{FAR}_A = 12\%$<br>$\text{IPR}_A = 0.96\%$ | $\text{FAR}_B = 0.35\%$<br>$\text{IPR}_B = 19\%$ | $\text{FAR}_C = 0.35\%$<br>$\text{IPR}_C = 0.96\%$ |

* Resort to a different verification procedure.

$$\text{FAR}_A = 0.05 + 0.07 - (0.05 \times .07) = 0.1165 = 12\%$$

$$\text{IPR}_A = 0.08 \times 0.12 = 0.0096 = 0.96\%$$

$$\text{FAR}_B = 0.05 \times 0.07 = 0.0035 = 0.35\%$$

$$\text{IPR}_B = 0.08 + 0.12 - (0.08 \times 0.12) = 0.1904 = 19\%$$

$$\text{FAR}_C = 0.05 \times 0.07 = 0.0035 = 0.35\%$$

$$\text{IPR}_C = 0.08 \times 0.12 = 0.0096 = 0.96\%$$

cated by an * on the Table) this should not be construed as a false alarm but simply as an indication of the need for further substantiation. Considered in this light, $FAR_c$ is 0.35 percent and $IPR_c$ is 0.96 percent.

## 5. Evaluation Criteria

There are several factors to be considered in evaluating personal identification systems for a particular application. In addition to the FAR and IPR discussed in the previous section, the following factors should be considered:

(1) Resistance to deceit

(2) Ease of counterfeiting an artifact

(3) Susceptibility to circumvention

(4) Time to achieve recognition

(5) Convenience to user

(6) Cost of recognition device and of its use

(7) Interfacing of device for intended purpose

(8) Time and effort involved in updating (adding and deleting users, issuing new passwords, keys, changing combinations).

(9) Processing required in computer system to support identification process.

(10) Reliability and Maintainability

(11) Cost of protecting the device.

(12) Cost of distribution and logistical support.

These factors will be discussed in the paragraphs which follow, the intent being to provide guidance on collecting and assessing information on specific personal identification systems. The evaluation of any given device should center on the experimental or analytic determination of these parameters.

### 5.1 Resistance to Deceit

The IPR indicates the extent to which a recognition device might allow acceptance of an imposter who was simply purporting to be an authorized individual. It is not intended to reflect cases in which an active effort at deceit is attempted. Such efforts might include attempts to mimic another person's voice, forge a signature, use a hand-shaped template, etc. It should be evident that any recognition device might be vulnerable to deceit by a sufficiently authentic-looking entity embodying a contrived set of input characteristics. Resistance to deceit would depend on the difficulty required to synthesize an entity having the necessary set of characterictics.

### 5.2 Counterfeiting of Artifacts

Recognition techniques which rely on artifacts, such as a key or plastic card, are vulnerable to being deceived by a counterfeit copy of the artifact. Here, the vulnerability is related to the uniqueness of the artifact. An artifact requiring very specialized and sophisticated equipment to produce, together with its encoded information, should be correspondingly difficult to counterfeit. It should be noted, however, that it may be possible to copy an artifact much more readily than to reproduce it by the original method. For example, some holographs can be copied by contact printing, without the need for a complex optical system or coherent light source. A further precaution should be noted with regard to ease of alteration. An artifact which might be difficult to produce initially might nevertheless be altered with less difficult, thereby allowing updating of a discarded or stolen artifact, or allowing an individual with a limited degree of access to masquerade as someone at a higher level. For example, assume that a card uses punched holes to establish the level of access. An unauthorized person might be able to plug some holes or to punch or file additional holes to gain access to a level other than the one authorized.

### 5.3 Susceptibility to Circumvention

Aside from deceiving a recognition device by some artificial means, consideration should be given to the ease with which the device might be circumvented altogether, without the need for deceiving the recognition logic. If the device has an output wire which carries the pass/reject signal, an obvious step would be to tap into this wire and inject a false pass signal. Other more subtle measures might be applied, depending on the manner in which the device operates and the way in which it functions in a system. It is evident that appropriate precautions must be taken to guard against such circumvention. One such precaution is the use of encryption, which is discussed in Section 6.5.

### 5.4 Time to Achieve Recognition

Different recognition schemes may require differing amounts of time to carry out the recognition process and arrive at a decision. This time is made up of the time required to actuate the device, which may involve keying in some data, such as a combanation, password, or personal identifier, the time for biometric sensing to take place, the time to manipulate an artifact, the time for a file retrieval to be carried out, the time for processing to occur, such as a correlation, the time for communication with a central facility, and finally the time to effect the acceptance or rejection. It may be necessary to allow for more than one trial, which further increases the time. In a system utilizing hand-written signatures, about 4 to 5 seconds is required for the signature itself; people are often not aware that it takes this long to sign their names. Systems which must be used frequently such as those needed to reverify authorization for multiple accesses, may have to work quite rapidly, although this speed requirement may not be compatible with the achievement of a high degree of certainty. User impatience with even moderate inconvenience imposed by security devices is well known, leading to such subterfuges as latches being taped and doors being propped open.

### 5.5 Convenience to User

For a personal identification system to gain acceptance, it must be reasonably convenient to the user; otherwise it would be regarded as an impediment and may even be circumvented by the user as suggested earlier [20]. For example, it should be evident that a system requiring inked fingerprint impressions for each recognition would be objectionable. However, an acceptable fingerprint impression for optical scanning can be obtained by placing the finger on the surface of a prism which is arranged to exploit the principle of frustrated total internal reflection.

Related to convenience is the ease of learning to actuate the recognition scheme, including data to be memorized such as passwords and combinations. The possibility for human error must be recognized and provisions made for starting over and repeating the process. These provisions should be limited, however, in order to deny an imposter the opportunity to gain acceptance through trial and error. Devices which depend on the actuation of buttons or keys in a coded sequence should be shielded so that a would-be imposter could not learn the sequence by observation.

A provision that can be included is a "time penalty", in which the recognition device is held off for a time interval after an unsuccessful identification attempt, in order to impede efforts to gain access by trial and error, especially by automated means. Also, an alarm indication can be generated when erroneous identification attempts are made, in order to call attention to possible intrusion attempts by an imposter.

### 5.6 Cost of Recognition Device

Some recognition devices are self-contained and can be used singly, while others require sophisticated support functions which are best performed centrally and shared among a number of devices. The support functions might require a specialized dedicated system, or they might be programmable on a general-purpose machine, in which case they could utilize a fraction of the processing capability of the system for which access protection is being provided. In any event, there will be a cost for each recognition device as installed at the points where identification is to be established, and there may be additional costs for centralized supporting equipment.

### 5.7 Interfacing of Device for Intended Purpose

The recognition device might be used for controlling access to an area or it might be used for controlling the use of equipment such as a terminal or operator's console. The recognition device must be suitably interfaced for the intended purpose and this may place certain constraints on the choice of device. The device should be interfaced in a manner which meets system requirements and which prevents the device from being disabled or circumvented. The installation should be tamper-proof, which involves physical integrity plus the use of alarm sensors which would be activated by attempts at circumvention. The device might be used for enabling local equipment and might also be tied to a central system which monitors its operation and which may provide support for the recognition process. The device may provide only a part of the acceptance process; the user might also have to employ supplementary procedures, which would generally be processed by a central system.

### 5.8 Time and Effort Involved in Updating

Good security practices entail periodic reissuing of the variable elements of the system —passwords, keys, combinations, encoded artifacts, etc. This should also be done if the system is suspected to have been compromised, such as through loss or theft of a key or artifact. Software-implemented provisions, such as passwords (including one-time passwords), may be relatively easy to change and to reissue, as compared to picture badges. Some push-button combination locks are designed to permit new combinations to be entered at will; locks and keys would be more difficult to update. The choice of an access control scheme would thus be influenced by how often updating would be required and the effort involved in carrying this out.

### 5.9 Processing Required in Computer System

As mentioned earlier, some recognition schemes involve data processing to support the recognition device. This processing, which could be performed on a general-purpose machine at a central location, may involve such tasks as retreiving profiles of user characteristics, comparing these against values obtained from the individual, coordinating multiple forms of access control, and performing the acceptance or rejection. These functions require computer programs, processing capacity, and storage in the central facility. These requirements could be significant where an attribute is represented by several hundred sampled values and a correlation must be performed between the file set and the "live" set. Routines for supporting the recognition devices would generally work in conjunction with other security programs in the central facility, such as those which establish access rights of users and device identity and which perform various monitoring functions.

### 5.10 Reliability and Maintainability

The reliability of a personal recognition device will have an important influence on the security of the system for which access control is being provided. Reliability may be defined as the probability that the device will perform its intended function over a specified interval of operation. A distinction should be made between the ability of the device to properly perform the required recognition function and its ability to perform dependably on a continuing basis. The ability to perform the recognition process correctly may be considered the device effectiveness, and is considered in determining the FAR and IPR. Reliability, as applied to equipment performance, refers to the ability to continue operating at the nominal level of effectiveness on a sustained basis without drifting out of tolerance or breaking down.

The personal identification equipment should be designed so that it is fail-safe, in that it should deny access if a failure occurs or if the power is cut off. It should be provided with detectors to warn against tampering. For maintenance purposes, there must be a method for disabling these protective circuits, but this method itself must be secure enough to prevent its being used in attempts at circumvention. The need for allowing multiple identification attempts was stated earlier; however, the number of retries should be limited to thwart an imposter who might try to gain access by trial and error.

### 5.11 Cost of Protecting the Device

With certain classes of devices, a knowledge of their internal working increases their vulnerability to being defeated. If such a device is easily stolen and carried off to be examined at leisure, the entire class of such devices could be compromised. Therefore, physical protection must be given these devices, and the cost of providing that protection must be weighed.

### 5.12 Cost of Distribution and Logistical Support

Studies indicate that costs for distribution and logistical support can exceed 20 percent of the total value of the contracted price of devices. A cost factor of this magnitude should be evaluated when devices are compared.

## 6. System Considerations

Each of the categories of authentication methods discussed has some degree of vulnerability. A password or the combination to a lock may be learned by another person. This could happen if a copy were left in some exposed location, or the user might secretly be observed while using it. In the case of a remote system, a password or any set of transmitted data might be obtained via a wiretap and then be used to gain unauthorized access. Artifacts, such as badges, cards and keys, can be stolen and used by an unauthorized person. If the loss is discovered, it may be possible to take steps to minimize the potential damage; however, a clever penetrator might appropriate the artifact only long enough to carry out a specific action and then return it without anyone's having been aware of its misuse. To protect against this threat, an auditing routine should be incorporated into the system which maintains records as to what is accessed, under what authentication, and for what purpose. Users of interactive, multiple-user systems should be provided with a detailed line-item register of every access, for whatever purpose to support user billings. Such session registers should include user I.D., system function being performed, clock item or System Resource Unit (SRU),[2] line-item cost and output terminal

[2] A System Resource Unit (SRU) is an entity used for accounting purposes, such as CPU seconds, disk tracks, and so forth.

receiving the data. The user should analyze the session registers against his access logs very carefully. This should enable the detection of unauthorized accesses, using properly designed and monitored controls.

Each of the categories of authentication methods discussed has some degree of vulnerability. Recognition systems based upon physiological attributes may be susceptible in varying degrees to circumvention. A voice recognition system depending upon a spoken password might be deceived by a recording of the unauthorized person. A picture pass might be altered or counterfeited to carry the picture of a would be penetrator in the place of an unauthorized individual, or a pentrator might disguise himself to resemble an authorized individual whose pass he had appropriated. It is possible to mold fingerprint impressions into thin rubber gloves which might be worn by a would-be penerator for the purpose of foiling a fingerprint matching system.

Even if an identification method could carry out its function entirely accurately and were immune to decit, it would still be necessary to assure that it could not be circumvented in some other way. For example, a recognition device might be used in conjunction with a remote terminal, requiring an enabling signal from the device to allow use of the terminal. A would-be penetrator might be able to falsify this signal, thus enabling the terminal without the need for recognition. Another form of circumvention might involve wiretapping, in which the circuit would be switched from the remote terminal to an intruder's terminal after the establishment of recognition and login by a legitimate user. In order to avert suspicion, the intruder could send a fictitious message to the legitimate user stating that the computer was temporarily out of service. It is thus evident that recognition techniques must be incorporated within complete systems where a hierarchy of provisions are made to assure overall system integrity. This could include the use of encryption for data and control signals.

### 6.1. Unauthorized Users Versus Unauthorized Usage

Within the context of system security, personal identification is employed to provide assurance that only authorized users are granted access to the system. Even if the personal identification scheme were 100 percent effective, however, there would still be certain risks and these require different kinds of safeguards. These risks are predominantly the following:

(1) Coercion of an authorized user to provide access for an unauthorized person. Coercion might take the form of a physical threat or some type of extortion.

(2) Collusion between an authorized user and an unauthorized person, possibly involving bribery.

(3) Performance of unauthorized actions by an authorized user either deliberately, for possible personal gain, or through error or carelessness.

It should be evident that simply assuring the correct identity of authorized users is not sufficient to counter the above threats. Other provisions must be included within the overall security program to safeguard against these threats. Some of these provisions are administrative, including the screening of individuals in the hiring process and in the granting of authorization, with periodic follow-up security checks, and the bonding of individuals in sensitive positions [7].

A full discussion of system security measures is beyond the scope of this Guideline; for further information, the reader is referred to *Computer Security Guidelines for Implementing the Privacy Act of 1974*, FIPS PUB 41 [18]. Additional references on controlled accessibility may be found in the *Controlled Accessibility Bibliography*, NBS Technical Note 780 [8]. However, certain system considerations which are closely related to personal identification are described briefly below.

### 6.2. Duress or Hostage Alarm

Protection can be provided for the case of an authorized individual being forced to gain access on behalf of an intruder. This is done by incorporating a secret procedure which would be invoked by the hostage in the process of seeking access to the system. It might be necessary to grant access to the system, in order to avert suspicion on the part of the intruder, so as not to jeopardize the hostage, but other security measures could be invoked, once the threat were made known. Many devices for personal identification include provisions for such a duress (or hostage) alarm.

### 6.3. Establishing and Checking Authorization

Control of access to system resources is governed by previously-established authorization. Authorization applies to the following factors:

(1) The set of individuals authorized to use the system,

(2) Data necessary to achieve personal identification,

(3) System resources (data files, programs, terminals, peripherals; also classes of activity: read-only, read/write, execute, search, transactions, program generation, privileged instructions),

(4) Data necessary for resource identification (such as identification code for a terminal),

(5) Authorization relationships between authorized individuals and system resources.

The process of establishing the above information is called authorization definition. Authorization checking is performed whenever access is attempted to the system or system resources.

### 6.4. Auditing of System Access

Provision should be made for the logging of accesses to a system in order to provide a record of who accessed the system, what was accessed, and what actions were performed. This information is useful in auditing system activities and in discovering and tracing possible intrusions. Logging is performed after an authorized access has been granted.

### 6.5. Encryption

Terminal security can be violated, despite controlled access to the terminal, by the use of wiretapping techniques. This could be done by using another terminal that poses as the authorized terminal by imitating its responses to the system. For this reason some method of protecting a system from such imposters is needed. The most effective technique is encryption of communications to and from the terminal.

Encryption is achieved either through a secret process (that is, the manner in which data is transposed and/or substituted) or through a commonly known process which depends on a secret parameter (called a "key") used by the process. In order to allow compatibility of encryption processes within the typical variety of network components, the latter method is preferred. The encryption process is generally specified in an algorithm (a set of rules or steps for performing a task). Decryption is the inverse process. Even with encryption, it might still be possible for an imposter to imitate encrypted responses of a fixed nature if they were always the same. However, it is a relatively simple matter in a system to use numbering schemes in the dialogue that would cause the responses to be encrypted in a manner that would be, in practice, impossible for an imposter to imitate.

The National Bureau of Standards has published an encryption algorithm which satisfies the primary technical requirements of a data encryption standard. This standard will be promulgated as Federal Information Processing Standard (FIPS) 46, Data Encryption Standard, dated 1977 January 15. The algorithm may be implemented in presently available electronic technology, using hardware developed for this purpose.

Control devices must be constructed to format the data for the encryption device and to transmit and receive the encrypted data. The design of these devices will depend on the terminal and the communication network to which it is attached.

Data encryption keys must be created and distributed to authorized personnel. They must be protected at all times and changed frequently. Periodic changes are suggested and immediate changes are necessary if a compromise is suspected to have occurred.

## Bibliography

[1] Autrey, Vaughn M., Will the Real Terminal User Please Stand Up, Telecommunications, May 1974, pp. 23-26.

[2] Beardsley, Charles W., Is Your Computer Insecure, IEEE Spectrum, January 1972, pp. 67-78.

[3] Branstad, D. K., Security Aspects of Computer Networks, AIAA Computer Network Systems Conference, Huntsville, Alabama, April 16-18, 1973.

[4] Cotton, Ira W., and Paul Meissner, Approaches to Controlling Personal Access to Computer Terminals, Proceedings of the 1975 Symposium Computer Networks: Trends and Applications, June 18, 1975, pp. 32-39.

[5] Doddington, George R., Speaker Identification for Entry Control, Proceedings of Wescon, 1975.

[6] Eleccion, Marce, Automatic Fingerprint Identification, IEEE Spectrum, September 1973, pp. 36-45.

[7] Parker, Donn D., Computer Security: Some Easy Things to Do, Computer Decisions. January 1974, pp. 17-18.

[8] Reed, Susan K., and Martha M. Gray, Controlled Accessibility Bibliography, National Bureau of Standards (U.S.), Tech. Note 780, 11 pages (June 1973).

[9] Reed, Susan K., and Dennis K. Branstad, Editors, Controlled Accessibility Workshop Report, National Bureau of Standards (U. S.), Tech. Note 827, 86 pages (May 1974).

[10] Rennick, R. J. and V. A. Vitols, MUFTI—A Multifunction Identification System, Proceedings of Wescon, 1975.

[11] Riganati, John P., An Overview of Electronic Identification Systems, Proceedings of Wescon, September 1975.

[12] Sternberg, Jacob, Automated Signature Verification Using Handwriting Pressure, Proceedings of Wescon, 1975.

[13] Stock, Robert M., Present and Future Identification Needs of Law Enforcement, Proceedings of Wescon, September 1975.

[14] Turn, Rein and Norman Z. Shapiro, Privacy and Security in Databank Systems—Measures of Effectiveness, Costs and Protection—Intruder Interactions, AFIPS Conference Proceedings, Fall Joint Computer Conference, Vol I, Part I, 1972, pp. 435-444.

[15] U. S. Department of Commerce, Experimental Statistics, M. G. Natrella, National Bureau of Standards Handbook 91, August 1963.

[16] U. S. Department of Commerce, Guidelines for Automatic Data Processing Physical Security and Risk Management, National Bureau of Standards (U.S.), FIPS PUB 31, 92 pages (June 1974).

[17] U. S. Department of Commerce, Index of Automated System Design Requirements as Derived from the OMB Privacy Act Implementation Guidelines, NBSIR 75-909, 14 pages (October 1975).

[18] U. S. Department of Commerce, Computer Security Guidelines for Implementing the Privacy Act of 1974, National Bureau of Standards (U. S.), FIPS PUB 41, 24 pages (May 1975).

[19] Warfel, George H., A Review of Personal Identification Systems, The Magazine of Bank Administration, December 1974, pp. 16-20.

[20] Warfel, George H., Personal ID Alternatives: Balancing Security and Economics Demands Harsh Compromises, Bank Systems and Equipment, September 1975, pp. 67-68.

[21] Wolf, Frank L., Elements of Probability and Statistics (McGraw Hill Book Co., 1962).

U. S. GOVERNMENT PRINTING OFFICE : 1977 O - 230-684

# NBS TECHNICAL PUBLICATIONS

## PERIODICALS

JOURNAL OF RESEARCH reports National Bureau of Standards research and development in physics, mathematics, and chemistry. It is published in two sections, available separately:

- Physics and Chemistry (Section A)

Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

- Mathematical Sciences (Section B)

Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

DIMENSIONS/NBS (formerly Technical News Bulletin)—This monthly magazine is published to inform scientists, engineers, businessmen, industry, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on the work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing.

Annual subscription: Domestic, $12.50; Foreign, $15.65.

## NONPERIODICALS

**Monographs**—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

**Handbooks**—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

**Special Publications**—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

**Applied Mathematics Series**—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

**National Standard Reference Data Series**—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a world-wide program coordinated by NBS. Program under authority of National Standard Data Act (Public Law 90-396).

NOTE: At present the principal publication outlet for these data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St. N.W., Wash. D. C. 20056.

**Building Science Series**—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

**Technical Notes**—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

**Voluntary Product Standards**—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The purpose of the standards is to establish nationally recognized requirements for products, and to provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

**Consumer Information Series**—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

*Order* **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.*

*Order* **following** *NBS publications—NBSIR's and FIPS from the National Technical Information Services, Springfield, Va. 22161.*

**Federal Information Processing Standards Publications (FIPS PUBS)**—Publications in this series collectively constitute the Federal Information Processing Standards Register. Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

**NBS Interagency Reports (NBSIR)**—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Services (Springfield, Va. 22161) in paper copy or microfiche form.

## BIBLIOGRAPHIC SUBSCRIPTION SERVICES

**The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:**

**Cryogenic Data Center Current Awareness Service.** A literature survey issued biweekly. Annual subscription: Domestic, $20.00; Foreign, $25.00.

**Liquified Natural Gas.** A literature survey issued quarterly. Annual subscription: $20.00.

**Superconducting Devices and Materials.** A literature survey issued quarterly. Annual subscription: $20.00. Send subscription orders and remittances for the preceding bibliographic services to National Bureau of Standards, Cryogenic Data Center (275.02) Boulder, Colorado 80302.